

## AMENDMENT

### In the Claims:

1           1.       (Once Amended) A method for facilitating the delegation of  
2       operations involved in providing digital signatures to a signature server, the  
3       method comprising:  
4           receiving a [request for a digital signature] message from a user at the  
5       signature server, the [request] message including an item to be signed on behalf of  
6       the user by the signature server;  
7           looking up a private key for the user at the signature server; and  
8           signing the item with the private key for the user[; and].  
9           [returning the signed item to the user so that the user can send the signed  
10      item to a recipient.]

1           2.       (Unchanged) The method of claim 1, wherein prior to signing the  
2       item, the method further comprises authenticating the user.

1           3.       (Unchanged) The method of claim 2, wherein prior to signing the  
2       item, the method further comprises determining whether the user is authorized to  
3       sign the item.

1           4.       (Unchanged) The method of claim 3, wherein determining whether  
2       the user is authorized to sign the item involves looking up an authorization for the  
3       user based upon an identifier for the user as well as an identifier for an application  
4       to which the user will send the signed item.

1           5.       (Unchanged) The method of claim 3, wherein determining whether  
2       the user is authorized to sign the item involves communicating with an authority  
3       server that is separate from the signature server.

1           6.       (Unchanged) The method of claim 1, further comprising allowing  
2 the user to authenticate the signature server prior to sending the [request] message  
3 to the signature server.

1           7.       (Once Amended) The method of claim 1, further comprising  
2 returning the signed item to the user so that the user can send the signed item to a  
3 recipient. [facilitating encryption of communications between the user and the  
4 signature server.]

AI  
1           8.       (Unchanged) The method of claim 1, wherein the method further  
2 comprises configuring the signature server to accommodate a new user by:  
3       receiving a request from an authorized entity to add the new user;  
4       generating a key pair for the new user, including a new user private key  
5 and a new user public key;  
6       communicating with a certification authority to obtain a certificate for the  
7 new user based on the key pair; and  
8       storing the certificate and the key pair for the new user in a location that is  
9 accessible by the signature server to enable the signature server to sign items on  
10 behalf of the new user.

1           9.       (Unchanged) The method of claim 1, wherein the method further  
2 comprises configuring the signature server to delete an old user by:  
3       receiving a request from an authorized entity to delete the old user;  
4       notifying a certification authority to revoke a certificate for the old user;  
5 and  
6       removing the private key for the old user from the signature server, so that  
7 the signature server can no longer sign items on behalf of the old user.

1           10.     (Once Amended) The method of claim 1, wherein the method  
2 further comprises archiving the [request] message and the signed item at the  
3 signature server.

1           11.     (Unchanged) The method of claim 1, wherein the method further  
2 comprises forwarding the signed item to an archive server in order to be archived.

A1  
1           12.     (Once Amended) A computer-readable storage medium storing  
2 instructions that when executed by a computer cause the computer to perform a  
3 method for facilitating the delegation of operations involved in providing digital  
4 signatures to a signature server, the method comprising:  
5           receiving a [request for a digital signature] message from a user at the  
6 signature server, the [request] message including an item to be signed on behalf of  
7 the user by the signature server;  
8           looking up a private key for the user at the signature server; and  
9           signing the item with the private key for the user[; and].  
10          [returning the signed item to the user so that the user can send the signed  
11 item to a recipient.]

1           13.     (Unchanged) The computer-readable storage medium of claim 12,  
2 wherein prior to signing the item, the method further comprises authenticating the  
3 user.

1           14.     (Unchanged) The computer-readable storage medium of claim 13,  
2 wherein prior to signing the item, the method further comprises determining  
3 whether the user is authorized to sign the item.

1           15.     (Unchanged) The computer-readable storage medium of claim 14,  
2 wherein determining whether the user is authorized to sign the item involves

3 looking up an authorization for the user based upon an identifier for the user as  
4 well as an identifier for an application to which the user will send the signed item.

1 16. (Unchanged) The computer-readable storage medium of claim 14,  
2 wherein determining whether the user is authorized to sign the item involves  
3 communicating with an authority server that is separate from the signature server.

1 17. (Once Amended) The computer-readable storage medium of claim  
2 12, wherein the method further comprises allowing the user to authenticate the  
3 signature server prior to sending the [request] message to the signature server.

1 18. (Once Amended) The computer-readable storage medium of claim  
2 12, wherein the method further comprises returning the signed item to the user so  
3 that the user can send the signed item to a recipient. [facilitating encryption of  
4 communications between the user and the signature server.]

1 19. (Unchanged) The computer-readable storage medium of claim 12,  
2 wherein the method further comprises configuring the signature server to  
3 accommodate a new user by:  
4 receiving a request from an authorized entity to add the new user;  
5 generating a key pair for the new user, including a new user private key  
6 and a new user public key;  
7 communicating with a certification authority to obtain a certificate for the  
8 new user based on the key pair; and  
9 storing the certificate and the key pair for the new user in a location that is  
10 accessible by the signature server to enable the signature server to sign items on  
11 behalf of the new user.

1           20.     (Unchanged) The computer-readable storage medium of claim 12,  
2 wherein the method further comprises configuring the signature server to delete an  
3 old user by:

4           receiving a request from an authorized entity to delete the old user;  
5           notifying a certification authority to revoke a certificate for the old user;  
6     and  
7           removing the private key for the old user from the signature server, so that  
8 the signature server can no longer sign items on behalf of the old user.

1           21.     (Once Amended) The computer-readable storage medium of claim  
2 12, wherein the method further comprises archiving the [request] message and the  
3 signed item at the signature server.

1           22.     (Unchanged) The computer-readable storage medium of claim 12,  
2 wherein the method further comprises forwarding the signed item to an archive  
3 server in order to be archived.

1           23.     (Once Amended) An apparatus that facilitates delegating  
2 operations involved in providing digital signatures, comprising:  
3           a signature server;  
4           a receiving mechanism within the signature server that is configured to  
5 receive a [request for a digital signature] message from a user, the [request]  
6 message including an item to be signed on behalf of the user by the signature  
7 server;  
8           a lookup mechanism within the signature server that is configured to look  
9 up a private key for the user; and  
10          a signing mechanism within the signature server that is configured to sign  
11 the item with the private key for the user[; and].

12 [a sending mechanism within the signature server that is configured to  
13 return the signed item to the user so that the user can send the signed item to a  
14 recipient.]

1 24. (Unchanged) The apparatus of claim 23, further comprising an  
2 authentication mechanism that is configured to authenticate the user prior to  
3 signing the item.

A, 1 25. (Unchanged) The apparatus of claim 24, further comprising an  
2 authorization mechanism that is configured to determine whether the user is  
3 authorized to sign the item prior to signing the item.

1 26. (Unchanged) The apparatus of claim 25, wherein the authorization  
2 mechanism is configured to determine whether the user is authorized to sign the  
3 item by looking up an authorization for the user based upon an identifier for the  
4 user as well as an identifier for an application to which the user will send the  
5 signed item.

1 27. (Unchanged) The apparatus of claim 25, wherein the authorization  
2 mechanism is configured to determine whether the user is authorized to sign the  
3 item by communicating with an authority server that is separate from the signature  
4 server.

1 28. (Unchanged) The apparatus of claim 23, further comprising an  
2 authentication mechanism that is configured to allow the user to authenticate the  
3 signature server prior to sending the [request] message to the signature server.

1 29. (Once Amended) The apparatus of claim 23, further comprising a  
2 sending mechanism within the signature server that is configured to return the

3 signed item to the user so that the user can send the signed item to a recipient. [an  
4 encryption mechanism that is configured to facilitate encryption of  
5 communications between the user and the signature server.]

1 30. (Unchanged) The apparatus of claim 23, further comprising an  
2 initialization mechanism that is configured to:  
3 receive a request from an authorized entity to add a new user;  
4 generate a key pair for the new user, including a new user private key and  
5 a new user public key;  
A1 6 communicate with a certification authority to obtain a certificate for the  
7 new user based on the key pair; and to  
8 store the certificate and the key pair for the new user in a location that is  
9 accessible by the signature server to enable the signature server to sign items on  
10 behalf of the new user.

1 31. (Unchanged) The apparatus of claim 23, further comprising a  
2 deletion mechanism that is configured to:  
3 receive a request from an authorized entity to delete an old user;  
4 notify a certification authority to revoke a certificate for the old user; and  
5 to  
6 remove the private key for the old user from the signature server, so that  
7 the signature server can no longer sign items on behalf of the old user.

1 32. (Once Amended) The apparatus of claim 23, further comprising an  
2 archiving mechanism that is configured to archive the [request] message and the  
3 signed item at the signature server.